23rd Mediterranean Conference on Control and Automation (MED)
June 16-19, 2015. Torremolinos, Spain

Effects of Permanent Bounded Cyber-Attacks on Networked Control Systems

Benjamin Gerard[1], Holger Voos[1], Yumei Li[1] and Mohamed Darouach[2]

***Abstract*— In this paper, the problem of permanent bounded cyber-attacks on networked control systems is treated. After a characterisation of malicious cyber attacks, the danger of permanent bounded cyber-attacks of two types is proved, the step attacks on system with invariant zero with zero real part and the free attacks. Simulation examples demonstrate the obtained results.**

***Index Terms*— Cyber-Attack, Geometric Approach, Malicious Attack, Permanent Attack, Invariant Zero, Networked Contol System.**

I. INTRODUCTION

Due to the increase of the use of the network in control systems, a new element has to be taken into account in their design: the security of your system w.r.t cyber attacks. You have to analyse the weakness of the networked communication to know the possible input and output losses, additions of deception signals. Networked Control Systems (NCSs) vulnerability to cyber-threats are regularly discovered [1]. Therefore, the security of NCSs become increasingly critical, which motivates our interest in the analysis on effects of the weakness of the networked communication, so as to be conscious of the possible consequences of malicious cyber-attacks.

Development of network, even more wireless technology, enable controlled system to receive/send data, measurements far from the controller. It may improve the performance or the flexibility of the system, but if you consider that hacking is possible, it increases the vulnerability to cyber attacks. When you design a system, you cannot know which networked sensor will be hacked, so you have to consider that they are all unsecured.

Malicious attacks, i.e stealthy and critical (see [2], [3], [4]) can be related to invariant set [5], output nulling subspace of linear system, invariant zero, controlled and condition invariants [6], [7], [8], the geometric approach [8] will be used in the cyber-attack context. The conditions enabling hackers to launch steathy attacks on a real system are studied. To avoid these conditions to happen, they have to be taken into account during the design procedure.

Recently, cyber-attacks on NCSs have currently attracted considerable attention. Some works were focused on perfectly attackable systems [2] and most of the cyber-attacks mentioned in literracy are exponential attacks [3], [9]. These attack can quickly reach saturations on states, controls or get far from a linearization point so that the system would stop to fulfill its linearity conditions. Moreover, these attacks can be detected since they are short term attacks which disrupt the system or launch emergency stop. The originallity of this work lies in its focus on permanent attacks with a limited but permanent impact on a NCS, which can be especially damaging, degrading product quality or energy consumption and thus rentability of a plant for instance. An extended malicious attacks formulation is proposed.

This paper is organized as follows. Problem statement, definitions and important theorem of the field are given in Section II. Then, the attack presention and possible protection, as a main contribution are described in Section III. Section IV shows examplesillustrating the danger of some permanent attacks. Finally, Section V concludes the paper.

Notation : $X^{\dagger}$ denotes pseudoinverse of X, $\mathcal{B}$ =Im(B), $\mathcal{C}$ = Ker(C), $< X|\mathcal{Y} >= \mathcal{Y} + X\mathcal{Y} + X^2\mathcal{Y} + \ldots + X^{n-1}\mathcal{Y}$, with $X \in \mathbb{R}^{n\times n}$ and $\mathcal{Y}$ subspace of $\mathbb{R}^n$.

II. PRELIMINARIES

A. System and problem statement

Let us consider linear systems of the following form

$$\left\{ \begin{array}{lcl} \dot{x}(t) & = & A_s x(t) + B_s u(t) + B_a a(t) \\ y(t) & = & C_s x(t) + D_a a(t) \end{array} \right. \quad (1)$$

where $x(t) \in \mathbb{R}^n$ is the state vector, y(t)$\in \mathbb{R}^{p_s}$ is the output, $u(t) \in \mathbb{R}^{m_s}$ is the vector of control inputs and $a(t) \in \mathbb{R}^{d_s}$ represents the attack on control inputs and/or measurement signals so with rank($[B_s \ B_a]$) = rank(B_s), rank($[C_s^T \ D_a^T]$) = rank(C_s) and Im(B_a) $\cap$ Im(D_a) = 0.The danger of a (B_a, D_a)-attack will be studied, but before system (1)will be simplified.

If $D_a = 0$, i.e the attacker do not falsify measurements to hide his attack. With $D_a \neq 0$, the original nullspace of C_s can be artificially augmented. To simply take into account D_a from the attacker point of view, we can settle C such that Im(C) = Im(C_s) $\cap$ Ker(D_a). If each $y_i(t)$ represent a real measurement, $D_a = \left[\begin{array}{cccccc} 0 & \ldots & 0 & C_{s_{k_1}}^T & \ldots & C_{s_{k_l}}^T \end{array} \right]^T$, $(k_1, \ldots, k_l) \in [1, p]t^l$, so we can define $C = \left[\begin{array}{ccc} C_{s_{k_{l+1}}}^T & \ldots & C_{s_{k_p}}^T \end{array} \right]^T$, $(k_{l+1}, \ldots, k_p) \in ([1, p] \setminus \{k_1, \ldots, k_l\})^{p-l}$. Other way to study attacked system as a strictly proper system ($D = 0$) can be found in Aling *et al* [8], [10]. In this paper, B_s will be neglected, A_s and the unhackable control inputs are considered giging a stable system, herein $A = A_s + B_s K$

*This work was supported by the Fund National de la Recherche, Luxemboug, under the project CO11/IS/1206050 (Sesanet).

[1]Benjamin Gerard, Yumei Li, Holger Voos are with Interdisciplinary Centre for Benjamin.gerard@uni.lu

[2] Mohamed Darouach is with the Centre de la Recherche en Automatique de Nancy (CRAN), Universite de Lorraine, France

is Hurwitz, this simplification is relevant as the effects on the remaining control inputs with corrupted measurement are treated in Mo [2] (attack on measurement only). For simplification, the following attacked part of the NCS in the sequel of the paper (with $B_a = B$) is studied:

$$\begin{cases} \dot{x}(t) &= Ax(t) + Ba(t) \\ y(t) &= Cx(t) \end{cases} \quad (2)$$

where A is Hurwitz, $x(t) \in \mathbb{R}^n$ is the state vector, y(t)$\in \mathbb{R}^p$ is the output, and $a(t) \in \mathbb{R}^d$ represents the attack on control inputs, $p \leqslant p_s$ and $d \leqslant d_s$. A goal of a hacker can be to find an attack $a(t)$ maximizing state effects (maybe reaching critical states or constant errors) and, ideally, such that $y(t) = 0, \forall t \leq 0$ or less than an ideal value as far as possible in order to keep detection from attack/fault detectors. Thus the following bounded permanent attack and the stealthy attack [3] can be defined.

Definition 1: A system is permanently boundly attackable if and only if $\forall\ T \in \mathbb{R}^{+*}$, $\forall\ \alpha \in \mathbb{R}^{+*}$, it exists a bounded attack signal $a(t)$ and a positive real T_1 such that $\forall\ t > T_1$, $||x||_{2,[t,t+T]} \geqslant \alpha$. $a(t)$ is called a bounded permanent attack.

Remark 1: The permanent bounded attack $a(t)$ reachs an effect : $||x||_2 > \alpha$ at least periodically, but for whatever chosen period.

Definition 2: [3] An attack signal $a(t), t \geqslant 0$, is $\varepsilon-$stealthy, if $\|y\|_\infty \leqslant \varepsilon$.

Undetectable attacks are studied, we recall one lemma and one theorem from Pasqualetti [4] (Lemma 3.1) and the fundamental lemma of geometric approach from Basile [8].

Lemma 1: For the system (1), the nonzero attack $a(t)$ is undetectable if and only if $y(x_1, a, t) = y(x_2, 0, t)$ for some initial state x_1, $x_2 \in \mathbb{R}^n$ and for all $t > 0$, or by linearity $y(x_0, a, t) = 0$ for $x_0 = x_1 - x_2$. $\triangledown$

Lemma 2: Any state trajectory $x_{|[t_0,t_1]}$ of (2) belongs to a subspace $\mathcal{L} \subseteq \mathbb{R}^n$ if and only if $x(t_0) \in \mathcal{L}$ and $\dot{x}(t) \in \mathcal{L}$ almost everywhere in $[t_0, t_1]$. $\triangledown$

B. Review of some geometrical results

For a given system, different categories of zeros exists and are related, as transmission, input-(and/or)-output-decoupling, blocking zeros. From a cyber attack point of view, invariant zeros defined as follows only will be considered.

Definition 3: $s_0 \in \mathbb{C}$ is an invariant zero of system (2): $rank \begin{bmatrix} s_0 I - A & -B \\ C & 0 \end{bmatrix} < n + min(d, p)$. (see [7])

Remark 2: For other definitions, which can be equivalent to definition 3 (for some conditions as minimality), you can read references [8], [11].

Now definitions of the geometric spaces [8], [6] can be given.

Definition 4: Consider a pair (A, B), a subspace $\mathcal{V} \subseteq \mathbb{R}^n$ is said to be an (A, B)-controlled invariant if $A\mathcal{V} \subseteq\ \mathcal{V} + \mathcal{B}$.

Definition 5: Consider a pair (A, C), a subspace $\mathcal{S} \subseteq \mathcal{X}$ is said to be an (A, C)-conditioned invariant if $A(\mathcal{S} \cap \mathcal{C}) \subseteq \mathcal{S}$, where $\mathcal{C} = KerC$.

Lemma 3: [8] A subspace $\mathcal{V} \subseteq \mathbb{R}^n$ is an (A, B)-controlled invariant if and only if there exists at least one matrix F such that $(A + BF)\mathcal{V} \subset \mathcal{V}$. $\triangledown$

- $\mathcal{V}^* = \max\mathcal{V}(A, \mathcal{B},\ \mathcal{C})$ the maximal (A, B)-controlled invariant contained in $\mathcal{C}$ and it is called the maximal output nulling invariant.
- $\mathcal{S}^* = \min\mathcal{S}(A, \mathcal{C},\ \mathcal{B})$ the minimal $(A, \mathcal{C})$-conditioned invariant containing $\mathcal{B}$.
- $\mathcal{R}^*$ the maximal outputnulling controllability subspace i.e $\mathcal{R}^* =< A + BF|\mathcal{B} \cap \mathcal{V}^* >$ [6], F from lemma 3.

$\mathcal{V}^*$ can be obtained with Algorithm 4.1.1 and 4.1.2 [8]. With an attack which is $0-$stealthy, $x(t)$ remains in the maximal output nulling invariant. Theorem of Antsakilis *et al* [7] on the $dim\mathcal{V}^*$ is recalled.

Theorem 1: $dim\mathcal{V}^* = q + dim\mathcal{R}^*$, with q the number of invariant zeros of the system (2).

Existence of invariant zeros (or $m < p$) ensures the existence of undetectable attack but not only as it will be detailed in the next section.

III. Attack and Protection

A. Malicious attack

Based on Basile and Marro work [8], (chapter 4, theorem 4.1.4 or 4.1.6), or Theorem 5.1 of Pasqualetti *et al.* [12], malicious attacks will be defined. We give two expressions for subspace $\mathcal{R}^*$ which is also the reachable set on $\mathcal{C}$, it can be obtained by different ways, $\mathcal{R}^*$ =$\mathcal{V}^* \cap \mathcal{S}^*$ but also $\mathcal{R}^*$ is the minimal $(A + BF)$-invariant containing $\mathcal{V}^* \cap \mathcal{B})$, with F a $\mathbb{R}^{m \times n}$-matrix such that $(A + BF)\mathcal{V}^* \subseteq \mathcal{V}^*$. So to be able to write a generic expression of output nulling inputs, the following lemma from Piziak[13] will be used,

Lemma 4: Let Γ and Λ be complex $m_2 \times m_1$ and $m_2 \times m_3$ matrices, respectively, with $m_1 < m_2$, $m_3 < m_2$. Then

$$2\Gamma\Gamma^\dagger[\Gamma\Gamma^\dagger + \Lambda\Lambda^\dagger]^\dagger\Lambda\Lambda^\dagger = \text{Orthohgonal Projection on } Im(\Gamma) \cap Im(\Lambda) \quad \triangledown$$

With V a basis of $\mathcal{V}^*$:

$$B_{\mathcal{V}*} = B^\dagger[BB^\dagger + VV^\dagger]^\dagger VV^\dagger \ \ and\ \ \overline{B}_{\mathcal{V}^*}R = B_{\mathcal{V}*} \quad (3)$$

where R is the matrix of the rank($B_{\mathcal{V}*}$)-first columns of the matrix of right singular vector. Whatever $v \in \mathbb{R}^{\text{rank}(B_{\mathcal{V}*})}$, $\overline{B}_{\mathcal{V}^*}v$ is a free part of output nulling control input as $B\overline{B}_{\mathcal{V}^*}v \subseteq \mathcal{V}^* \cap \mathcal{B}$ thanks to lemma 4.

A change of basis enhance the structure of a given system. $P = \begin{bmatrix} P_1 & P_2 & P_3 \end{bmatrix}$ with Im(P_1) = $\mathcal{R}^*$, Im($[P_1\ P_2]$) = $\mathcal{V}^*$ and P_3 such that P is invertible. In the new basis, with a control input/attack $a(t) = FTx'(t) + a'(t)$ (F such that $\mathcal{V}^*$ $(A + BF)$-invariant see lemma 3) system (2) becomes

$$A' = P^{-1}AP = \begin{bmatrix} A'_{11} & A'_{12} & A'_{13} \\ 0 & A'_{22} & A'_{23} \\ 0 & 0 & A'_{33} \end{bmatrix}, \quad (4)$$

$$B'^T = T^{-1}B = \begin{bmatrix} B'_{11} & B'_{12} \\ 0 & 0 \\ 0 & B'_{32} \end{bmatrix}, C' = CT = \begin{bmatrix} 0 & 0 & C'_3 \end{bmatrix}.$$

The two first subspaces are unobservable (thanks to state feedback $Fx(t)$ or originally. The first one is controllable

but to be part of the state that can be freely driven, we must have $\mathcal{V}^* \cap \mathcal{B} \neq 0$. $a'(t)^T = \begin{bmatrix} v(t)^T & w(t)^T \end{bmatrix}$ and $B'_{11} = T^{-1}\overline{B}_{\mathcal{V}^*}$. The second one is the subspaces linked with invariant zero, A'_{22} is a squarre matrix of size q (see Th.1).

Link with the kalman decomposition can be settled:

- Uncontrollable and Unobservable modes are invariant zeros with $F = 0$.
- Controllable and Unobservable modes "are" in $\mathcal{R}^*$.
- Uncontrollable and observable modes "are" neither invariant zeros, nor in $\mathcal{R}^*$.
- Controllable and observable modes may be or not be moved in a unobservable subspace via a state feedback.

Theorem 2: $a(t)$ is a continuous 0-stealthy attack if and only if it exists an $(A+BF)$-controlled invariant $\mathcal{W} \subseteq \mathcal{V}^*$, $a(t) = Fx(t) + \overline{B}_{\mathcal{W}} v(t)$ where $\overline{B}_{\mathcal{W}}$ is a matrix of full column rank such that $\text{Im}(B\overline{B}_{\mathcal{W}}) \subseteq \mathcal{W}$. ▽

Proof: **(if)** As $\mathcal{W} \subseteq \mathcal{V}^*$ a similar proof to [12] is straightforward and a similar structure to (4) can be obtained. **(only if)** a is considered as a continuous 0-stealthy i.e undetectable attack, so from lemma 1, $\exists\ x_0$ such that $y(x_0, a, t) = 0$. We note $\mathbb{W} = \{x(x_0, a, t), t > 0\}$ and $\overline{\mathcal{W}} = span(\mathbb{W})$ and also note $\mathbb{A} = \{a(t), t > 0\}$ and $\mathcal{A} = span(\mathbb{A})$. $B_{\mathcal{A}}$ is the basis of $\mathcal{A}$ and thus $\exists\ \lambda$ function from t to $\mathbb{R}^{\dim(\mathcal{A})}$, $a(t) = B_{\mathcal{A}}\lambda(t)$. $\mathcal{W}$ is defined as the maximal $(A, \text{Im}(BB_{\mathcal{A}}))$-controlled invariant contained in $\mathcal{C}$, so $\exists$ matrix F_1 such that $(A + BB_{\mathcal{A}}F_1)\mathcal{W} \subseteq \mathcal{W}$. As $\mathcal{W} \subseteq \mathcal{C}$, $\mathcal{W} \subseteq \mathcal{V}^*$. We can write $a(t) = B_{\mathcal{A}}F_1x(t) + B_{\mathcal{A}}\lambda(t) - B_{\mathcal{A}}F_1x(t) = Fx(t) + B_{\mathcal{A}}v(t)$, with $B_{\mathcal{A}}$ full column rank, $F = B_{\mathcal{A}}F_1$ and $v(t) = \lambda(t) - F_1x(t)$. From the fundamental lemma 2, as a is continuous, $\dot{x}(t) \in \text{Im}(\mathcal{W})$, as $(A + BB_{\mathcal{A}}F_1)x(t) \in \text{Im}(\mathcal{W})$, $\text{Im}(BB_{\mathcal{A}}) \subseteq \mathcal{W}$. ■

In theorem 2, it is shown that the malicious attack of [12] can have a more various presentation, using a subspace of $\mathcal{V}^*$. For instance, if with measurement takeover, a subspace $\mathcal{W}$ is unobservable, $\overline{B}_{\mathcal{W}}v(t)$ are malicious attacks.

B. Permanent attacks

If only $Fx(t)$ part of the malicious attack is considered, the attacker has to proceed with state feedback so he has to be able to design a functional observer to reconstruct $Fx(t)$. Nevertheless seeing this attack with the invariant zero (s_0) point of view, the control input can be built with no knowledge on the state thank to the structural knowledge of the system; it can be seen as an open loop attack. A invariant zero based attack has to have some specific initialisation conditions. (which are automatically satisfied with a state feedback). Knowing the invariant zero s_0, the attacker could search for the null space $\mathcal{K}$ of $\begin{bmatrix} s_0I - A & -B \\ C & D \end{bmatrix}$ and obtain $\mathcal{K} = \text{span}\left\{\begin{bmatrix} x_0^T & a_0^T \end{bmatrix}\right\}$, x_0 is the state-zero direction and a_0 is the input-zero direction, then the input $a(t) = \lambda a_0 \mathcal{R}e(\mathrm{e}^{s_0 t})$ couls be settled, so

$$x(t) = e^{At}x(0) + \int_0^t e^{A(t-\tau)}Ba(\tau)d\tau$$
$$= e^{At}(x(0) - \lambda x_0) + e^{At}\lambda x_0 + \int_0^t e^{A(t-\tau)}Ba(\tau)d\tau \quad (5)$$

$x_f(t) = e^{At}x(0)$ is the attack-free system behavior, $x_a(t) = e^{At}\lambda x_0 + \int_0^t e^{A(t-\tau)}Ba(\tau)d\tau$ is the zero based attack behavior, so $Cx_a(t) = 0$, thus the anomaly due to the fact that the attack does not fulfilled the initialisation condition is $-Ce^{At}\lambda x_0$. If we consider that $x(0) = 0$, with the attack $a(t)$, the output can be written : $y = -Ce^{At}\lambda x_0$. As whatever vector in $\left\{\lambda \begin{bmatrix} x_0^T & a_0^T \end{bmatrix}, \lambda \in \mathbb{R}\right\}$ can be choosen to settle the attack, so with a λ small enough detection become impossible.

Theorem 3: If system (2) has at least one invariant zero with zero real part, $\forall\ \varepsilon > 0$, the system is permanently boundly attackable with a ε-stealthy attack.

With x_0 the state-zero direction, $\lambda = \varepsilon/(2||Cx_0||\gamma)$ and $\delta = \frac{ln(\frac{\varepsilon+2||C\lambda x_0\gamma||}{\varepsilon})}{\zeta}$ where γ and ζ such that $||e^{At}|| \leqslant \gamma e^{-\zeta t}$, we define $a(t) = \sum_{i=0}^{l} a_{t_k}(t)$ consisting in a finite sum of attacks of the form $a_{t_i}(t) = \begin{cases} 0 & t < t_i \\ \lambda a_0 \mathcal{R}e(e^{s_0(t-t_i)}) & t \geqslant t_i \end{cases}$, with $t_i = i\delta$, $a(t)$ is called a step attack. ▽

Proof: First if the system has an invariant zero s_0 with zero real part, $\exists\ (x_0, a_0)$ with $\begin{bmatrix} s_0I - A & -B \\ C & D \end{bmatrix}\begin{bmatrix} x_0 \\ u_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$. λ, for a given ε is defined as follows : $\lambda = \varepsilon/(2||Cx_0||\gamma)$. Moreover as A is a Hurwitz, $\exists\ (\gamma, \zeta) \in \mathbb{R}^{2*+}$, $||e^{At}|| \leqslant \gamma e^{-\zeta t}$. For a given ε, we define $\delta = \frac{ln(\frac{\varepsilon+2||C\lambda x_0\gamma||}{\varepsilon})}{\zeta} \Rightarrow ||C\lambda x_0||\gamma\frac{e^{-\zeta\delta}}{1-e^{-\zeta\delta}} \leqslant \frac{\varepsilon}{2}$. We consider the attack $a(t) = \sum_{i=0}^{l} a_{t_k}(t)$ consisting in a finite sum of attacks of the form $a_{t_i}(t) = \begin{cases} 0 & t < t_i \\ \lambda a_0 \mathcal{R}e(e^{s_0(t-t_i)}) & t \geqslant t_i \end{cases}$, with $t_i = i\delta$. If $s_0 = 0$, $a(t)$ is a step function, if $s_0 = ib$, $a(t)$ is a sinus where its amplitude is a step function. For $t \in [t_0, t_1]$, $||y(t)|| \leqslant ||C\lambda x_0||\gamma e^{-\zeta t} \leqslant \varepsilon/2 \leqslant \varepsilon$. For $t \in [t_i, t_{i+1}]$, recurrently,

$$||y(t)|| \leqslant ||C\lambda x_0||\gamma(e^{-\zeta t} + \sum_{k=1}^{i} e^{-k\zeta\delta})$$
$$\leqslant ||C\lambda x_0||\gamma(e^{-\zeta t} + \frac{e^{-\zeta\delta}}{1 - e^{-k\zeta\delta}}) \leqslant \varepsilon/2 + \varepsilon/2 \leqslant \varepsilon$$

So the attack is ε-stealthy. The attack $a(t)$ is contructivly bounded, and, for a given α, it exists a real T_1 such that $\forall t > T_1,\ ||x||_{2,[t,t+T]} \geqslant \alpha$ with well chosen l i.e well chosen number of steps. ■

Theorem 4: If system (2) has no invariant zero with positive real part and $\overline{B}_{\mathcal{V}^*} \neq 0$ with $\overline{B}_{\mathcal{V}^*}$ defined in (3), the system is permanently boundly attackable with a ε-stealthy attack. $a(t) = Fx(t) + \overline{B}_{\mathcal{V}}v(t)$ is called a free attack. ▽

Proof: Straightforward from define of $\overline{B}_{\mathcal{V}^*}$ with constant v, $y(t)$=0 and $||x_\infty||$ is proportional to $||v||$ as A stable. ■

C. Security Measure

The system designer has to be careful with the data communicated via the network, (for supervision for instance). Decreasing transmitted data or at least real time transmitted data increases security on the system. Data transmission interception enable hacker to identify more accuratly the system which could help him to launch stealthy attacks as they can need a good knowledge of the aimed system. Multiplying sensors, even with low accuracy, i.e cheap, enable to increase the hacking difficulties.

The design of the system is critic from a security perspective. Some hardware particularities will impact the invariant zeros sets, sets defined with respect to the considered hacked signals. The communication choices for control inputs and measurement outputs will affect the ability for an attacker to create some unobservable attacks. Avoiding zeros and even more with zero real part seem to be the first step of the protection against permanently bounded attacks.

Invariant zeros are very sensitive toward uncertain parameters. If these parameters can be modulated on our system, invariant zeros variations could enable to detect attacker unaware of these variations. Nevertheless attacker can develop robust attack when he is able to get enough information.

IV. Examples based on the four tanks system

First the nonlinear form of the four tanks system [14] is given

$$\begin{cases} \dot{h}_1 = -\frac{s_1}{S_1}\sqrt{2gh_1} + \frac{s_3}{S_1}\sqrt{2gh_3} + \frac{\gamma_1 k_1}{S_1}u_1 \\ \dot{h}_2 = -\frac{s_2}{S_2}\sqrt{2gh_2} + \frac{s_4}{S_2}\sqrt{2gh_4} + \frac{\gamma_2 k_2}{S_2}u_2 \\ \dot{h}_3 = -\frac{s_3}{S_3}\sqrt{2gh_3} + \frac{(1-\gamma_2)k_2}{S_3}u_2 \\ \dot{h}_4 = -\frac{s_4}{S_4}\sqrt{2gh_4} + \frac{(1-\gamma_1)k_1}{S_4}u_1 \end{cases} \quad (6)$$

with $y = [h_1; h_2]$, h_i are water levels, S_i and s_i are sections (tanks and pipes), g is the standard gravity, k_i are the gains of pump, u_i are pump voltages and γ_i are dispatching parameters. Second a linearized version of this system [14] around the point $(h_1^0, h_2^0, h_3^0, h_4^0)$ is obtained.

$$\begin{cases} \dot{x} = \begin{bmatrix} -f_1 & 0 & S_3 f_3/S_1 & 0 \\ 0 & -f_2 & 0 & S_4 f_4/S_2 \\ 0 & 0 & -f_3 & 0 \\ 0 & 0 & 0 & -f_4 \end{bmatrix} x \\ \quad + \begin{bmatrix} \gamma_1 k_1/S_1 & 0 \\ 0 & \gamma_2 k_2/S_2 \\ 0 & (1-\gamma_2)k_2/S_3 \\ (1-\gamma_1)k_1/S_4 & 0 \end{bmatrix} a \\ y = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} x \end{cases} \quad (7)$$

with $x_i = h_i - h_i^0$, $a_i = u_i - u_i^0$ where $f_i = \frac{s_i}{S_i}\sqrt{\frac{g}{2h_i^0}}$

The location of the zeros of this system depends on the parameters γ_1 and γ_2, $S_1 = S_3 = 28$, $S_2 = S_4 = 32$, $s_1 = s_3 = 0.071$, $s_2 = s_4 = 0.057$, $g = 981$.

A. A by-step Attack

By setting $\gamma_1 = \gamma_2 = 0.5$, $h_1^0 = 13.039$, $h_2^0 = 20.23$, $h_3^0 = 3.279$, $h_4^0 = 5.027$, $u_1^0 = u_2^0 = 3.4$, $k_1 = 3.33$ and $k_2 = 3.35$, we obtain a zero located at the origin. As explained in section III-B, the by-step attack can be effective, with this zero, as it has no imaginary part, the step attack represented in figure is used. The effects of this input on the water levels of the four tanks linearised system can be visualize in Fig.1b for the linearized model and in Fig.1c. The divergence of states 3 and 4 can be seen whereas states 1 and 2, the measured ones, remain at a very low level. This level can be arbitrarly low by choosing the step amplitude of the control input. Obviously, the smaller the step is, the slower the divergence is, but with stealthiness time is not a constraint for the attack.

B. Free attack

Now parameters of the four tanks system are settled as follows: $h_1^0 = 12.262$, $h_2^0 = 12.7825$, $h_3^0 = 1.634$, $h_4^0 = 1.409$, $u_1^0 = u_2^0 = 3$, $k_1 = 3.33$, $k_2 = 3.35$.

An additional attack is added on sensors: $D_a = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ (see system (1)), which lead to study the system (7) with the single output $y(t) = x_1(t)$ ($y_2(t)$ corrupted is ignored, see section II-A). Malicious attacks are of the form :

$$a(t) = \begin{bmatrix} a_1(t) \\ a_2(t) \end{bmatrix} = \begin{bmatrix} 0 & 0 & -A_3 f_3/(\gamma_1 k_1) & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} a_f(t).$$

Applying a stepped attack $a_f(t)$ i.e a step $a_2(t)$ as in Fig2a as permanently bounded attack, the consequences on the water level are as presented in Fig.3b which could be detected with redundant sensor on state x_2, x_3 or x_4. The same attack signal $a(t)$ on the real nonlinear system (6) gives the water level showed in Fig.2c, as the attack is low $||u(t)|| < 0.11$, the linearization condition are still rather respected and so $|h_1(t) - h_1^0|$ remains low. With a higher attack (see Fig.3a), the undetectability on the linearized model remain perfect whereas with a nonlinear model, effects on h_1 cannot be neglected as it can be seen in Fig.3c.

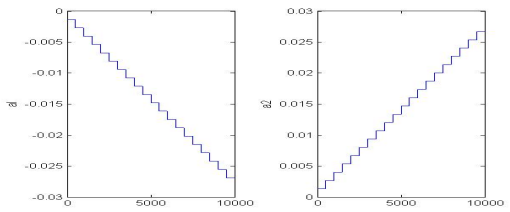
V. Conclusion

This paper enhanced the possibility hopefully with relatively strict assumptions and the danger of permanently bounded attacks. Sufficient conditions have been provided for the existence of two different kinds of these attacks, the step attack and the free attack. Taking into account these conditions enables system designer to avoid these attacks. The danger of each attack (step and free) are shown to be real via two numerical examples. Futher works lead us to analyse the danger of zero with a "little" real part.

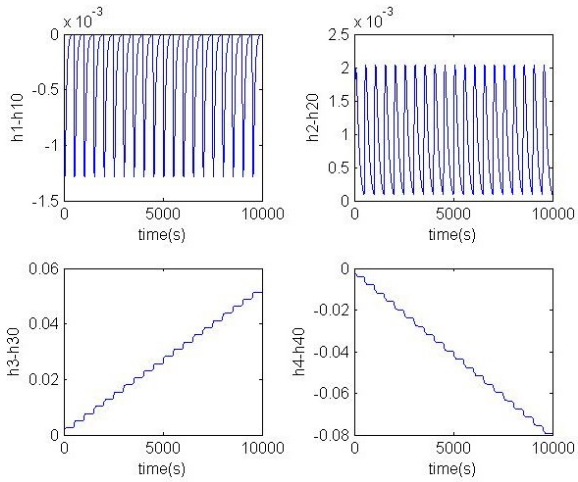
References

[1] [Online]. Available: https://ics-cert.us-cert.gov/alerts.

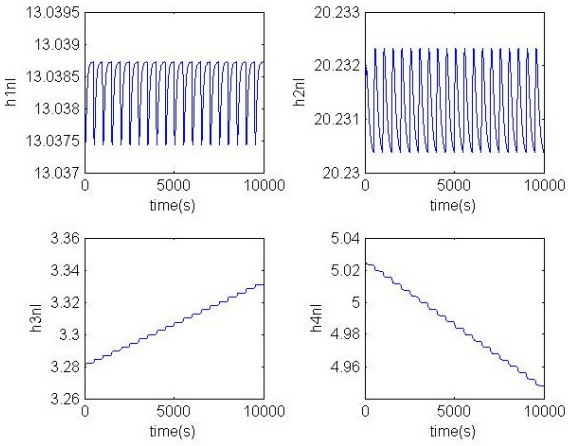
[2] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *First Workshop on Secure Control Systems, Cyber Physical Systems Week 2010*, April 2010.



(a) Step Inputs



(b) Water levels of the four tanks with linear model



(c) Water levels of the four tanks with nonlinear model

Fig. 1: Invariant Zero Attack : null zero

[3] A. Teixeira, I. Shames, H. Sandberg, and K. Johanson, "Revealing stealthy attacks in control systems," in *50th Annual Allerton Conference*, October 2012.

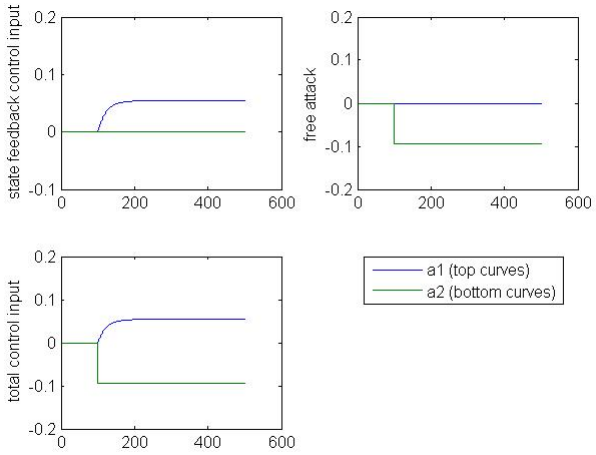
[4] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Aut. Control*, vol. 58, 2013.

[5] A. Rosich, H. Voos, Y. Li, and M. Darouach, "A model predictive approach for cyber-attack detection and mitigation in control systems," in *Decision and Control (CDC), 2013 IEEE 52st Annual Conference on*, December 2013.

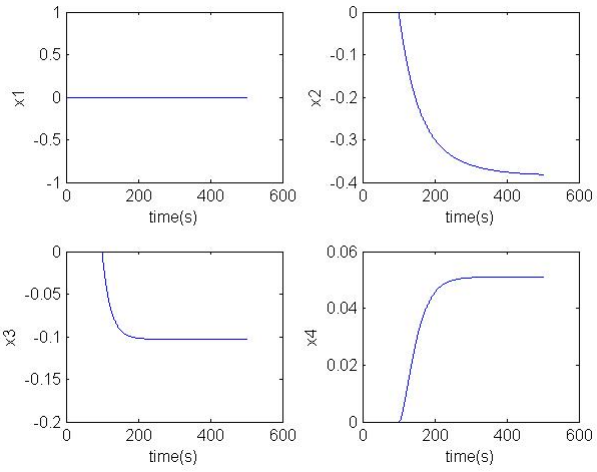
[6] B. Anderson, "Output nulling invariant and controllability subspaces," in *Proc. Triennal IFAC World Congress*, 1975.

[7] P. J. Antsaklis and T. W. C. Williams, "On the dimension of the supremal (a,b)-invariant and controllability subspaces," *IEEE Trans. Aut. Control*, vol. 6, 1980.

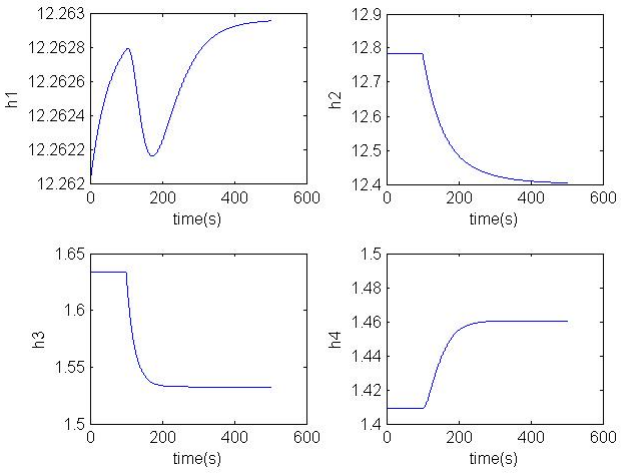
[8] G. Basile and G. Marro, *Controlled and Conditioned Invariants in Linear System Theory*. Englewood Cliffs, New Jersey: Prentice Hall,



(a) Control Inputs

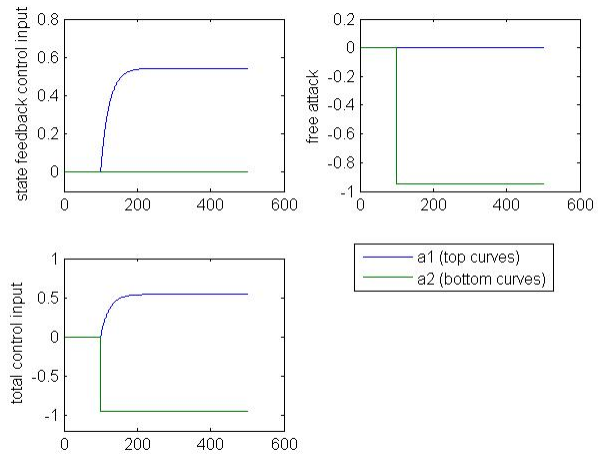


(b) Water levels of the four tanks (linear model)

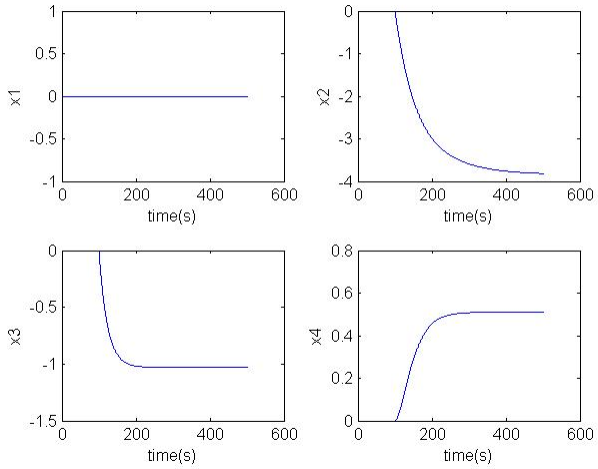


(c) Water levels with low input attack (nonlinear model)

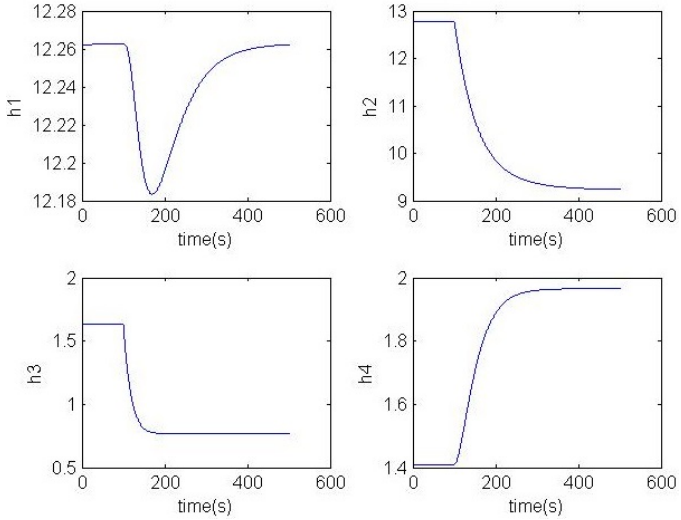
Fig. 2: Low Free attack on the four tanks system



(a) Control Inputs



(b) Water levels with high input attack (linear model)



(c) Water level with high input attack (nonlinear model)

Fig. 3: High Free attack on the four tanks system

1992.

[9] Y. Li, H. Voos, and M. Darouach, "Robust $calH_\infty$ cyber-attacks estimation for control systems," (Nanjing, China), 2014.

[10] H. Aling and J. Schumacher, "A nine-fold canonical decomposition for linear systems," *Int. J. Contr.*, vol. 39, pp. 779–805, 1984.

[11] J. Tokarzewski, "On a geometric characterisation of zeros for non-square linear systems with time-delay in state," *International Journal of Systems Science*, vol. 42, pp. 2035–2043, 2010.

[12] F. Pasqualetti, F. Dörfer, and F. Bullo, "Cyber-physical security via geometric control: Distributed monitoring and malicious attacks," in *Proc. IEEE Conf. Decision & Control*, (Maui, HI, USA), 2012.

[13] R. Piziak, P. Odell, and R. Hahn, "Constructing projections on sums and intersections," *Computer and mathematics with applications*, vol. 37, pp. 67–74, 1999.

[14] K. H. Johansson, "The quadruple-tank process: A multivariable laboratory process with an adjustable zero," *IEEE Trans. Aut. Control*, vol. 8, 2000.